GOVERNMENT OF INDIA
FINANCE
LOK SABHA

STARRED QUESTION NO:25
ANSWERED ON:03.02.2017
Online Frauds
Giluwa Shri Laxman;Gogoi Shri Gaurav

Will the Minister of FINANCE be pleased to state:

(a) whether the Government has set up the Central Fraud Registry for investigating the frauds committed in the banks and through ATM/Debit/Credit cards and if so, the details thereof;
(b) whether there has been a spurt in financial frauds using mobile phones, internet banking and digital transactions etc. in the past few months particularly during and after demonetization and if so, the details thereof;
(c) the number of fraudulent transactions detected by the above Registry and the result of the investigation carried out thereon; and
(d) the steps taken/being taken by the Government to ensure foolproof e-transactions and also protect customers from the said frauds?

Answer

THE MINISTER OF FINANCE

(a) to (d) : A Statement is laid on the table of the House.

****

Statement as referred in reply to part (a) to (d) of Lok Sabha Starred Question No. *25 for answer on 03.02.2017 regarding Online Frauds tabled by SHRI LAXMANGILUWA and SHRIGAURAV GOGOI, MPs.

(a) to (d): In January 2016, Central Fraud Registry (CFR) has been operationalized at Reserve Bank of India (RBI) as searchable online central fraud data base for use by the banks in respect of frauds above Rs.1 lakh. The CFR contains critical aspects/ information, including modus operandi in respect of frauds as reported by the banks and select Financial Institutions (FIs). This data base is helpful to the banks not only during credit decisions but also to know about fraud in various areas of banking including cyber frauds, ATM/debit/ credit card and internet banking.

All the banks/select FIs have been given access rights through user ids and password. The CFR helps the banks and FIs in detecting frauds in their organisation based on the frauds reported by other banks/FIs in respect of any particular constituent of the bank. It is the primary responsibility of the banks/FIs to detect the fraud with or without using CFR and comply with RBI regulation with regard to classification and reporting of frauds.

RBI has given the following details of fraud reported in credit cards/ ATM/Debit Cards and Internet Banking categories for the first three quarters of 2016:
Details of frauds reported in Credit Cards/ ATM/Debit Cards and Internet Banking Categories (Amount in Lakh ?)

Quarter Year 2016 Credit Cards ATM/ Debit Cards Internet Banking Total (All three categories)
No. of Frauds Amount No. of Frauds Amount No. of Frauds Amount No. of Frauds Amount
June 1927 714.94 1328 611.76 18 60.6 3273 1387.3
September 1626 733.59 1511 760.08 19 52.7 3156 1546.37
December 1004 708.25 1225 528.96 31 44.88 2260 1282.09
Total 4557 2156.78 4064 1900.8 68 158.18 8689 4215.76

The measures initiated by the RBI to prevent cyber related frauds is given below:
(i) RBI has issued circular on 'Skimming of ATM/Debit/Credit Cards' ,vide DBS.Co.FrMC.No.17968/23.10.001/2005-06 dated June 26, 2006, advising banks to take various preventive measures to combat frauds relating to skimming or duplicating of credit cards. The banks, inter alia, were also advised to advise customers not to reveal PIN in response to requests received through e-mail, to periodically verify the transaction history to ensure its correctness, if any unauthorized transaction was observed it should be immediately reported to the bank and inform the bank if the card is lost or stolen.
(ii) Caution advices are also issued by RBI as and when necessary for preventing and controlling the frauds. Three caution advices have been issued recently in connection with (i) Fraud in Mobile Application (CA No. 4097) (ii) ATMs-Large value cash shortages-Malware attacks (CA No. 4087) and (iii) Fraud-Letter of Comfort -Buyers Credit -Misuse of SWIFT messaging system CA No.(4094).
(iii) RBI has reiterated its instructions vide circular DBS.CO.CFMC.BC.No.6/23.04.001/2016-17 dated September 28, 2016 on funds transfer requirement received through email/fax messages. Banks were advised to strengthen the mechanism put in place by them in

this regard and also to adhere to it strictly, including contacting the customer over phone at his registered phone number to ensure genuineness of request of the customer.

(iv) In order to focus more attention on IT related matters, Reserve Bank of India has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015. RBI has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security. The banks are required, among other things, to have a cyber-security policy, cyber crisis management plan, gap assessment vis-Ã -vis the baseline requirements indicated in the circular, monitoring certain risk indicators in the area, report unusual cyber security incidents within 2 to 6 hours, ensure board involvement in the matter and robust vendor risk management. The progress of banks in scaling up their cyber security preparedness is monitored.

(v) RBI carries out IT Examination of banks separately from the regular financial examination of banks from last year. This report has a special focus on cyber security. The reports have been issued to the banks for remedial action. RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond to and recover from the incidents. Department of Banking Supervision also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of Indian Computer Emergency Response Team (CERT-In). RBI also has set up an IT subsidiary, with a focus, among other things, on cyber security within RBI as well as in regulated entities.

*****